CLAIMS

What is claimed is:

1. In a routing device, a method of operation comprising:

receiving a packet sent by a client device destined for a server;

independently determining whether said packet is a part of a conversation between the client and the server based at least in part on persistent information included in said packet; and

handling the packet based at least in part on the result of said independent determination.

2. The method of claim 1, wherein said independent determination comprises independently verifying a conversation identifier included in said packet based at least in part on other information included in said packet.

3. The method of claim 2, wherein said independent verification comprises

independently regenerating the conversation identifier using at least said other information included in said packet; and

comparing the independently re-generated conversation identifier with the included conversation identifier.

4. The method of claim 3, wherein said conversation identifier is a nonce, and said independent re-generation comprises independently re-generating the nonce using a deterministic function with a sequence number of the nonce and a plurality

of persistent field values extracted from the packet, and a pre-provided secret value as inputs to the deterministic function.

5. The method of claim 4, wherein said plurality of persistent field values comprise one or more of a source address, a destination address and a port number.

6. The method of claim 4, wherein the method further comprises at least one of receiving into said routing device said secret value, and equipping/configuring said routing device with said deterministic function.

7. The method of claim 4, wherein said independent generation is performed using a selected one of a message authentication code function and an universal hash function.

8. The method of claim 4, wherein the method further comprises recording a time of first observation for the nonce if the nonce is a newly observed nonce.

9. The method of claim 8, wherein the method further comprises determining if time has elapsed more than a predetermined threshold since a time of first observation was recorded for the nonce, if the extracted nonce and the independently generated nonce are deemed to be the same.

10. The method of claim 1, wherein the method further comprises forwarding the packet to the server if the packet is deemed to be a part of a conversation between

the client device and the server, and non-forwarding the packet if the packet is deemed not a part of a conversation between the client device and the server.

11. In a server, a method of operation comprising:

generating an independently verifiable conversation identifier for a packet destined for a client device, using at least persistent information that will be included in said packet;

including the independently verifiable conversation identifier with said packet for use by the client device to include in a subsequent packet sent by the client device destined for the server; and

transmitting said independently verifiable conversation identifier included packet to said client device.

12. The method of claim 11, wherein said generation of an independently verifiable conversation identifier comprises:

generating a sequence number for a nonce; and

generating the nonce as the independently verifiable conversation identifier for the packet using a deterministic function with the sequence number, a plurality of persistent field values of the packet, and a secret value as input values to the deterministic function.

13. The method of claim 12, wherein said plurality of persistent field values comprise one or more of a source address, a destination address and a port number.

14. In a client device, a method of operation comprising:

receiving a packet a from a server;

extracting from the packet at least an independently verifiable conversation identifier included in the packet by the server for inclusion in a subsequent packet of the client device for the server, to allow one or more intermediate routing devices to be able to independently determine whether to permit continuing forwarding of the subsequent packet of the client device to the server; and

saving said extracted at least independently verifiable conversation identifier for said subsequent use.

15. The method of claim 14, wherein the method further comprises

retrieving at least a saved independently verifiable conversation identifier;

including the retrieved independently verifiable conversation identifier in a packet to be sent to the server; and

transmitting the independently verifiable conversation identifier included packet to the server.

16. The method of claim 14, wherein said extracting comprises extracting an included nonce and an associated sequence number of the nonce, the nonce being independently verifiable by a party using a deterministic function and having knowledge of a secret value, based on persistent information included the packet.

17. A routing apparatus comprising:

an interface to receive a packet sent by a client device destined for a server; and

a function unit coupled to the interface to independently determine whether said packet is a part of a conversation between the client and the server based at

least in part on persistent information included in the packet, and output a packet disposition signal based at least in part on the result of said independent determination.

18. The routing apparatus of claim 17, wherein said function unit is to designed to make said independent determination by independently verifying a conversation identifier included in said packet based at least in part on other information included in said packet.

19. The routing apparatus of claim 18, wherein said function unit comprises

an identifier generator to independently regenerate the conversation identifier using at least said other information included in said packet; and

a comparator coupled to the identifier generator to compare the independently re-generated conversation identifier with the included conversation identifier.

20. The routing apparatus of claim 19, wherein said conversation identifier is a nonce, and said identifier generator is designed to independently re-generate the nonce using a deterministic function with a sequence number of the nonce and a plurality of persistent field values extracted from the packet, and a pre-provided secret value as inputs to the deterministic function.

21. The routing apparatus of claim 20, wherein said identifier generator comprises a deterministic function.

22. A server comprising:

at least one processor; and

a communication interface coupled to the processor to transmit packets to one or more client devices on behalf of the processor including

a generator to generate an independently verifiable conversation identifier for a packet destined for one of said one or more client devices, using at least persistent information that will be included in said packet,

a summing unit to insert the independently verifiable conversation identifier with said packet for use by the particular client device to include in a subsequent packet sent by the client device destined for the server and

a transmitter to transmit said independently verifiable conversation identifier included packet to said particular client device.

23. The apparatus of claim 22, wherein said generator comprises

a counter to generate a sequence number for a nonce; and

a deterministic function unit to generate the nonce as the independently verifiable conversation identifier for the packet using the sequence number, a plurality of persistent field values of the packet, and a secret value as input values.

24. The apparatus of claim 23, wherein said plurality of persistent field values comprise one or more of a source address, a destination address and a port number.

25. The apparatus of claim 23, wherein said deterministic function is a selected one of a message authentication code function and an universal hash function .

26. A client device comprising:

a processor; and

a communication interface coupled to the processor to send and receive packets on behalf of the processor, including

a transceiver to receive a packet a from a server,

an extractor coupled to the transceiver to extract from the packet at least an independently verifiable conversation identifier included in the packet by the server for inclusion in a subsequent packet of the client device for the server, to allow one or more intermediate routing devices to be able to independently determine whether to permit continuing forwarding of the subsequent packet of the client device to the server, and save said extracted at least independently verifiable conversation identifier for said subsequent use.

27. The client device of claim 26, wherein the communication interface further comprises a function unit to retrieve at least a saved independently verifiable conversation identifier, and insert the retrieved independently verifiable conversation identifier in a packet to be sent by said transceiver to the server.

28. The client device of claim 26, wherein said extractor is designed to extract an included nonce and an associated sequence number of the nonce, the nonce being independently verifiable by an intermediate party using a deterministic function and having knowledge of a secret value, based on persistent information included the packet.